Wise Information Security for collaborating e-Infrastructures

Recent activities of the WISE Security for Collaborating Infrastructures (SCI) working group

David Groep (Nikhef, NL), David Kelsey (UKRI-STFC,UK), Maarten Kremers (SURF, NL)

ISGC2023, Taipei, 21 March 2023

In collaboration with and co-supported by EU H2020 EOSC Future, GN4-3 & GN5-1

https://wise-community.org

Thank you - WISE collaborators in 2021-23

Sincere thanks are due to the following for their collaboration:

- Ana Afonso, Tom Barton, Vincent Brillault, Ian Collier, Linda Cornwall, Bob Cowles, David Crooks, Barbara Krašovec, Sven Gabriel, Baptiste Grenier, David Groep, Nicole Harris, Jens Jensen, Urpo Kaila, David Kelsey, Daniel Kouril, Maarten Kremers, Mikael Linden, Alf Moens, Ian Neilson, Ralph Niederberger, Mischa Salle, Hannah Short, Adam Slagell, Uros Stevanovic, Romain Wartel, Chris Weaver, Jule Ziegler
- And colleagues in EGI, WLCG, IRIS, GridPP, EUDAT, XSEDE, HBP, GEANT, GN4-3, GN5-1, EOSC, IGTF, REFEDs, FIM4R, SIG-ISM, Trusted CI
  - And many others in the past
- These individuals have done the work!
  - *And many apologies to any missed*

Contents

- The WISE Community
- Security for Collaborating Infrastructures Working Group (SCI-WG)
    - SCI Trust Framework
    - SCI maturity assessment and guidance
    - AARC PDK maintenance in WISE SCI-WG
        - New template Security Operations Security Policy
        - Data protection and GDPR
        - Community Security Policy
- Future plans for WISE and SCI-WG

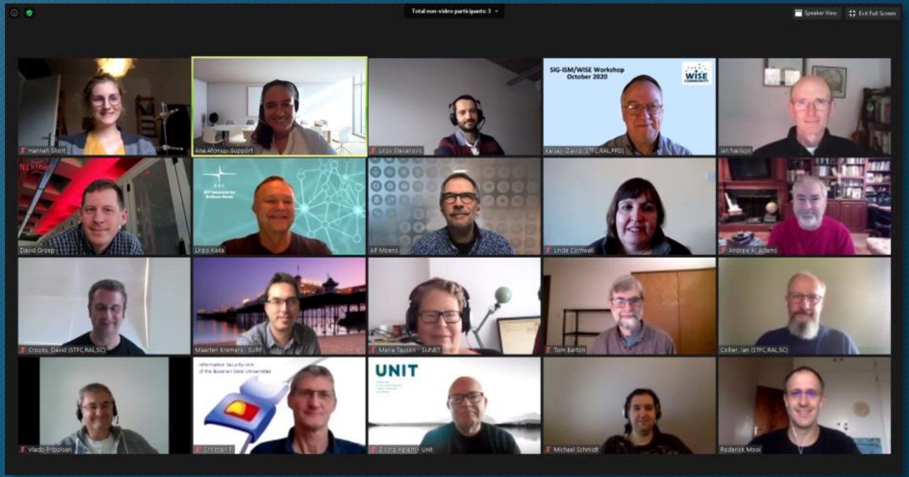
- See most recent "WISE" talk at ISGC2021 for more details about WISE working groups *https://indico4.twgrid.org/event/14/contributions/313/*

The WISE Community

- Started in October 2015 – Joint - GEANT SIG-ISM & IGTF SCI
- Community members come from e-Infrastructures across the world
- WISE meetings 2019-22
  - LITNET – Kaunas, Lithuania – April 2019 (joint with SIG-ISM)
  - NSF Cybersecurity Summit, San Diego, USA – Oct 2019 (last time in person)
  - Five virtual meetings during COVID-19 pandemic
    - April 2020, Oct 2020, May 2021, Oct 2021, April 2022
    - All joint with GEANT SIG-ISM
- There was no full WISE Community meeting in autumn 2022
  - Difficult to work on trust and policy when not together in person
  - WISE SCI working group continued to meet (virtually) for much of 2022

Some recent WISE meetings

San Diego, CA, USA – Oct 2019
All attendees at NSF Cybersecurity Summit



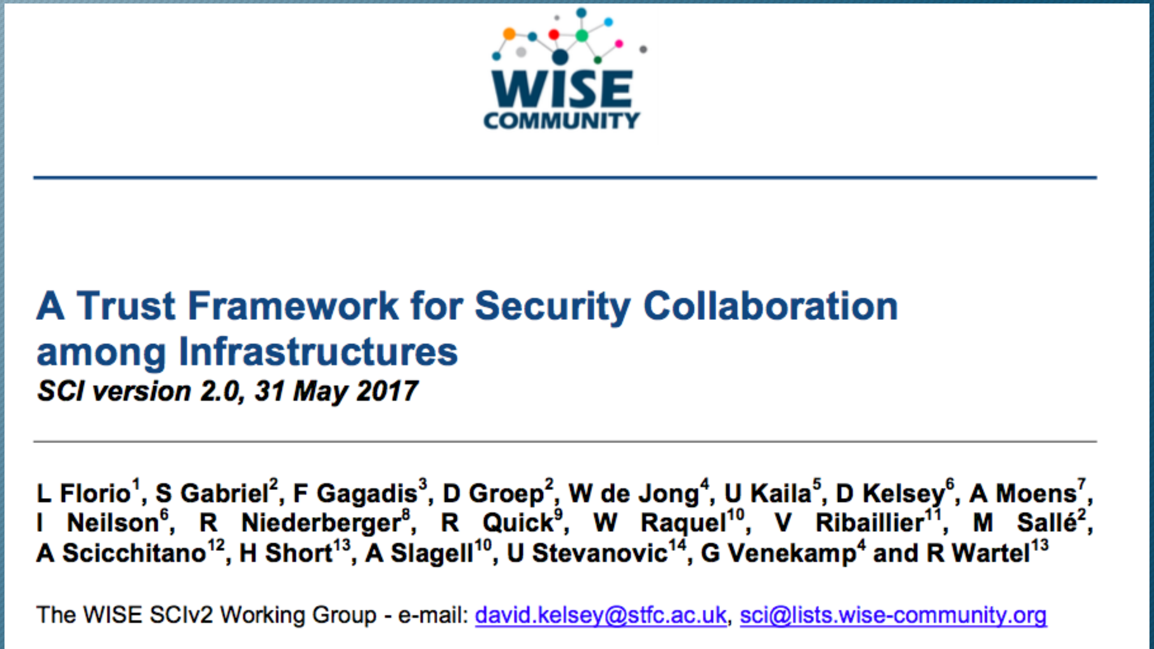
Virtual – Oct 2020
Joint with SIG-ISM

Security for Collaborating Infrastructures - The WISE SCI working group (SCI-WG)

SCI-WG - Shared threats & shared users

- Infrastructures are subject to many of the same threats
  - Shared technology, middleware, applications and users
- User communities use multiple e-Infrastructures
  - Often using same federated identity credentials
- Security incidents often spread by following the user
  - E.g. compromised credentials
- e-Infrastructure security teams need to collaborate
  - Trust is required

SCI Version 2 – published 31 May 2017 (TNC17) (version 1 was published at ISGC2013)



A Trust Framework for Security Collaboration among Infrastructures

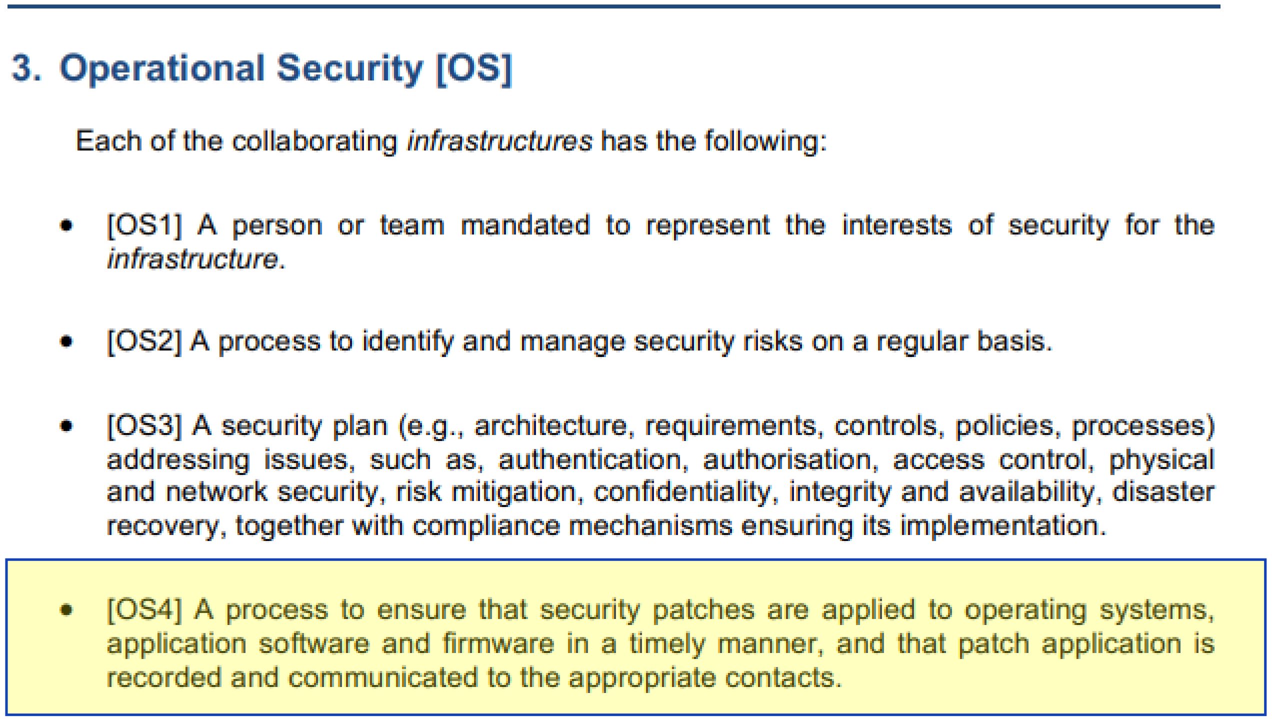
SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

A Trust Framework for Security Collaboration among Infrastructures

- https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf



3. Operational Security [OS]

Each of the collaborating *infrastructures* has the following:

- [OS1] A person or team mandated to represent the interests of security for the *infrastructure*.
- [OS2] A process to identify and manage security risks on a regular basis.
- [OS3] A security plan (e.g., architecture, requirements, controls, policies, processes) addressing issues, such as, authentication, authorisation, access control, physical and network security, risk mitigation, confidentiality, integrity and availability, disaster recovery, together with compliance mechanisms ensuring its implementation.
- [OS4] A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts.

□ 29 Assertions across 5 Categories.

□ How to assess the level of compliance?

Security for Collaborating Infrastructures …

- Self Assessment of maturity
  - against SCI Trust Framework
- Was presented as “work in progress” at ISGC2021
  - Guidance was completed in 2021-22

Science and Technology Facilities Council

WISE COMMUNITY

WISE SCI v2 maturity assessment - ‘how-to’ guide update

At SIG-ISM - WISE Workshop, 21 April 2022
(and updated after publication in May 2022)

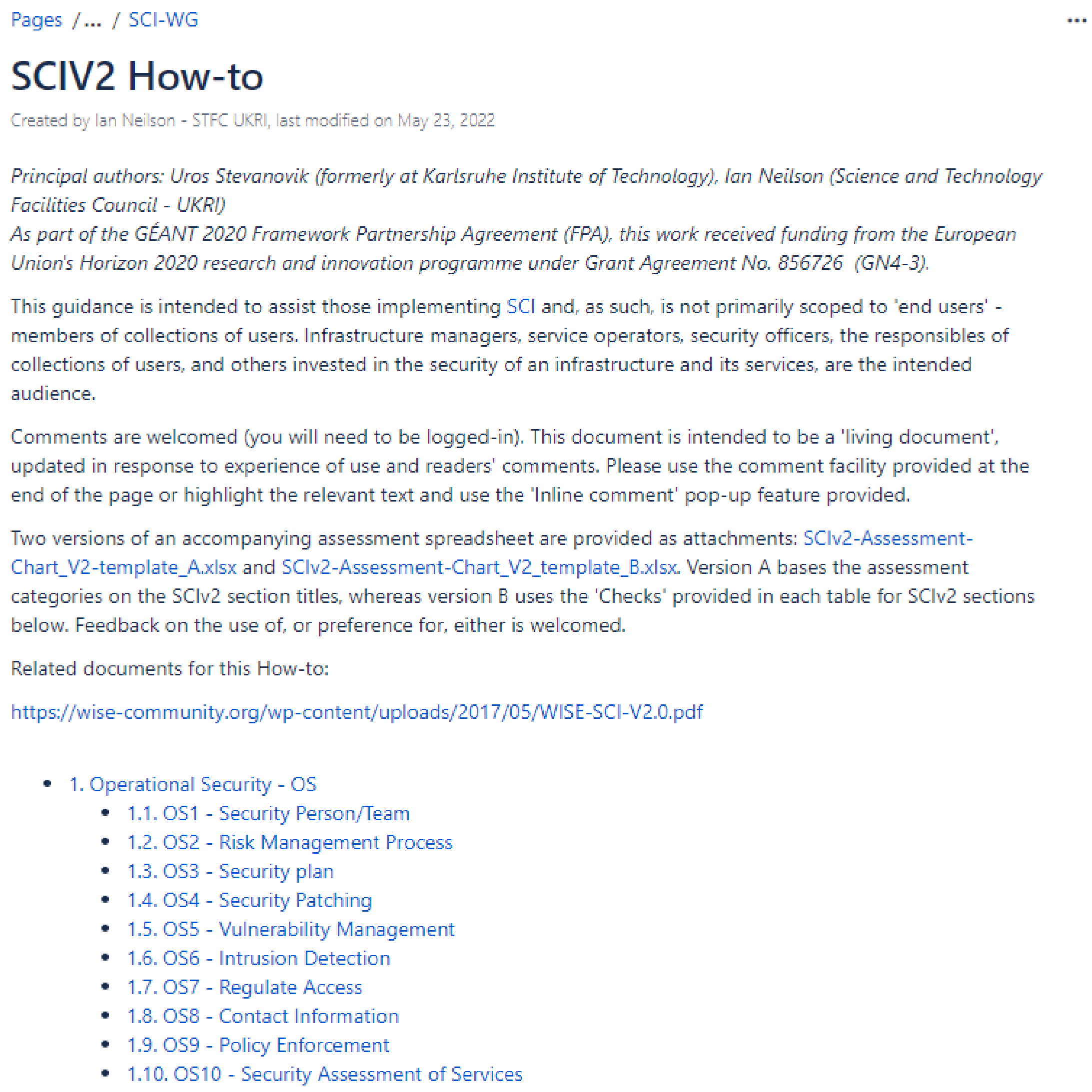
Ian Neilson (UKRI-STFC)

WISE words ….

- WISE SCI v2 Trust Framework
- draft guidance documents
- draft maturity assessment spreadsheets

Work was completed in May 2022

- All information now in one place on the WISE Wiki:
- https://wiki.geant.org/display/WISE/SCIV2+How-to



Pages / … / SCI-WG

SCIV2 How-to

Created by Ian Neilson - STFC UKRI, last modified on May 23, 2022

Principal authors: Uros Stevanovik (formerly at Karlsruhe Institute of Technology), Ian Neilson (Science and Technology Facilities Council - UKRI)
As part of the GÉANT 2020 Framework Partnership Agreement (FPA), this work received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

This guidance is intended to assist those implementing SCI and, as such, is not primarily scoped to 'end users' - members of collections of users. Infrastructure managers, service operators, security officers, the responsibles of collections of users, and others invested in the security of an infrastructure and its services, are the intended audience.

Comments are welcomed (you will need to be logged-in). This document is intended to be a 'living document', updated in response to experience of use and readers' comments. Please use the comment facility provided at the end of the page or highlight the relevant text and use the 'Inline comment' pop-up feature provided.

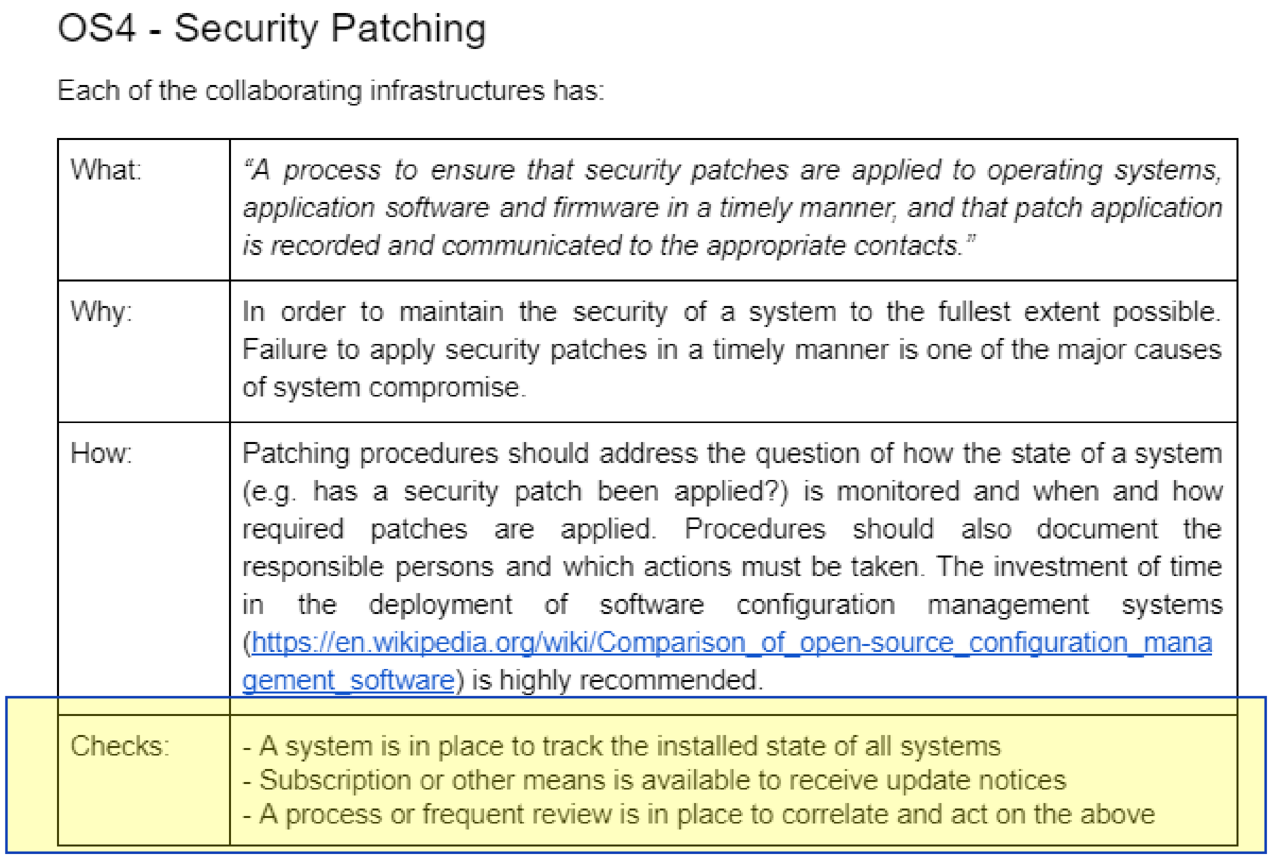
Two versions of an accompanying assessment spreadsheet are provided as attachments: SCIv2-Assessment-Chart_V2-template_A.xlsx and SCIv2-Assessment-Chart_V2_template_B.xlsx. Version A bases the assessment categories on the SCIv2 section titles, whereas version B uses the 'Checks' provided in each table for SCIv2 sections below. Feedback on the use of, or preference for, either is welcomed.

Related documents for this How-to:

https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

SCI v2 How-To

- To provide guidance on interpreting the SCIv2 text
- *https://wiki.geant.org/display/WISE/SCIV2+How-to*



OS4 - Security Patching

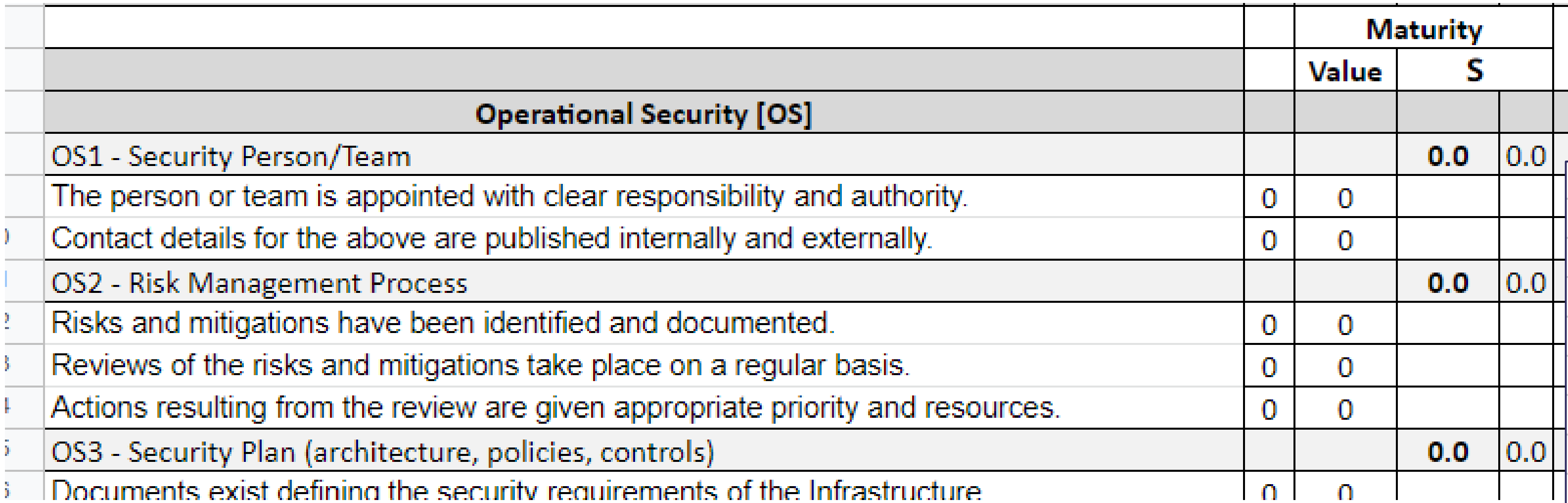
Each of the collaborating infrastructures has:

What:	*"A process to ensure that security patches are applied to operating systems, application software and firmware in a timely manner, and that patch application is recorded and communicated to the appropriate contacts."*
Why:	In order to maintain the security of a system to the fullest extent possible. Failure to apply security patches in a timely manner is one of the major causes of system compromise.
How:	Patching procedures should address the question of how the state of a system (e.g. has a security patch been applied?) is monitored and when and how required patches are applied. Procedures should also document the responsible persons and which actions must be taken. The investment of time in the deployment of software configuration management systems (https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software) is highly recommended.
Checks:	- A system is in place to track the installed state of all systems - Subscription or other means is available to receive update notices - A process or frequent review is in place to correlate and act on the above

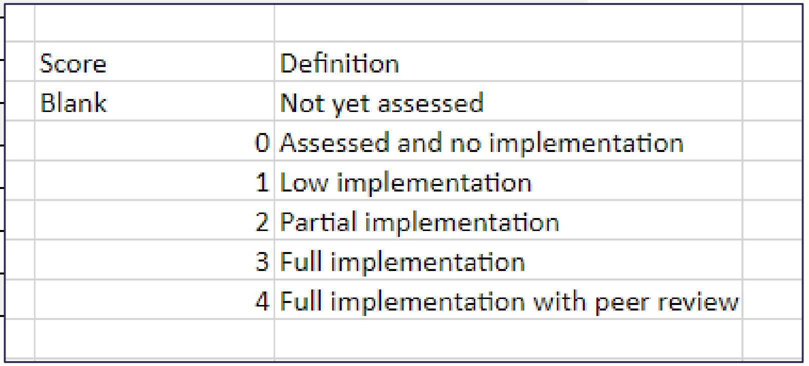
WISE COMMUNITY

SCIv2 Assessment Chart (B)

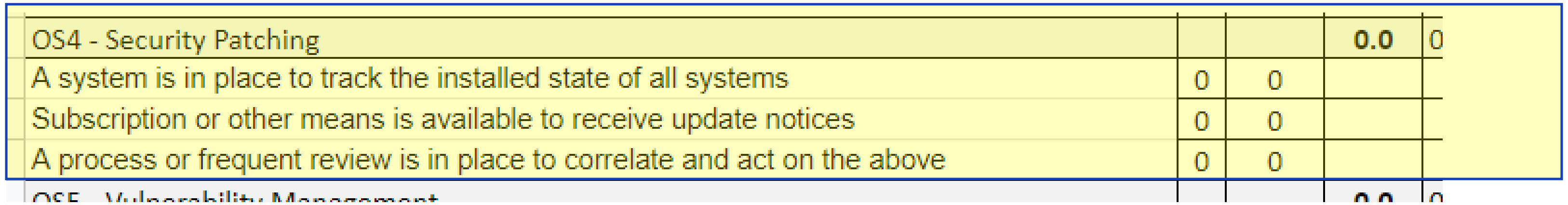
- https://wiki.geant.org/download/attachments/440303650/SCIv2-Assessment-Chart_V2_template_B.xlsx?api=v2



		Maturity			Evidence (Document Name and/or URL)
		Value	S		
Operational Security [OS]					
OS1 - Security Person/Team			0.0	0.0	
The person or team is appointed with clear responsibility and authority.	0	0			
Contact details for the above are published internally and externally.	0	0			
OS2 - Risk Management Process			0.0	0.0	
Risks and mitigations have been identified and documented.	0	0			
Reviews of the risks and mitigations take place on a regular basis.	0	0			
Actions resulting from the review are given appropriate priority and resources.	0	0			
OS3 - Security Plan (architecture, policies, controls)			0.0	0.0	
Documents exist defining the security requirements of the Infrastructure	0	0			



Score	Definition
Blank	Not yet assessed
0	Assessed and no implementation
1	Low implementation
2	Partial implementation
3	Full implementation
4	Full implementation with peer review



OS4 - Security Patching			0.0	0
A system is in place to track the installed state of all systems	0	0		
Subscription or other means is available to receive update notices	0	0		
A process or frequent review is in place to correlate and act on the above	0	0		
OS5 - Vulnerability Management			0.0	0

Science and Technology Facilities Council

Security for Collaborating Infrastructures …

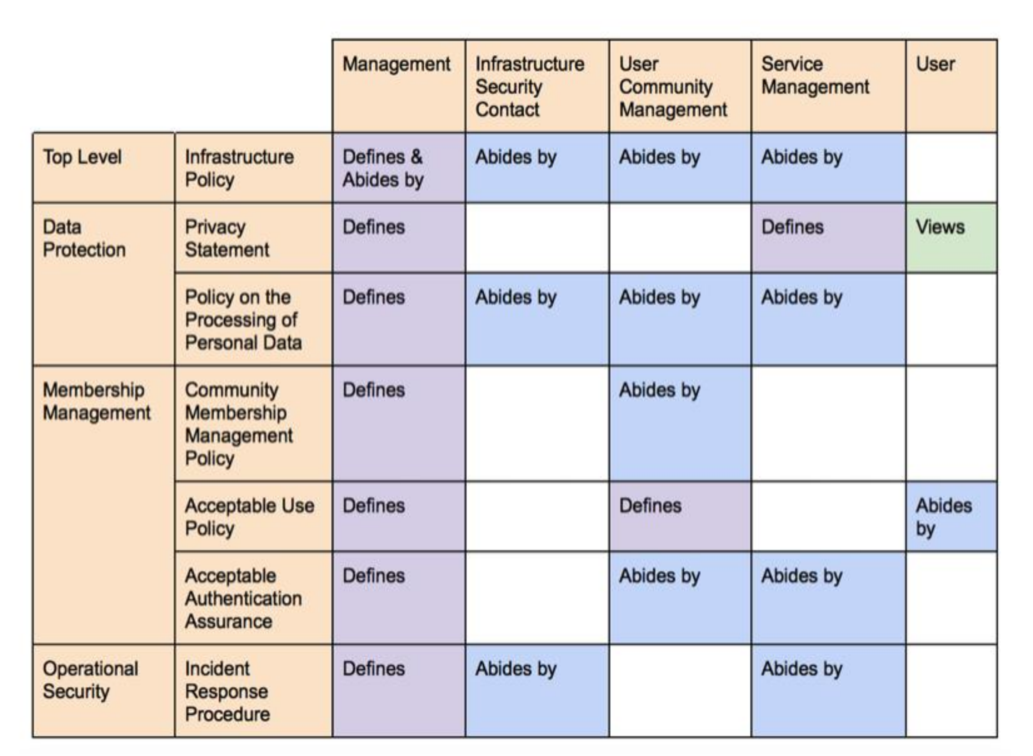
- Developing the AARC Policy Development Kit (updating baseline templates)

Development of AARC PDK by WISE SCI-WG

- Policy templates are useful to new Infrastructures and help build trust and interoperability (as compliant with SCI Trust Framework)
- Involve experience from many Infrastructures and policy groups (including AEGIS) https://aarc-project.eu/about/aegis/
- WISE SCI-wg will collect feedback from Infrastructures
  - And use this if/when a new version of a template is required
- Unlike AUP, new templates may contain optional components
  - Infrastructures just use the components that work for them

Building on AARC PDK in WISE SCI-WG

https://aarc-project.eu/policies/policy-development-kit/



		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	
Data Protection	Privacy Statement	Defines			Defines	Views
	Policy on the Processing of Personal Data	Defines	Abides by	Abides by	Abides by	
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

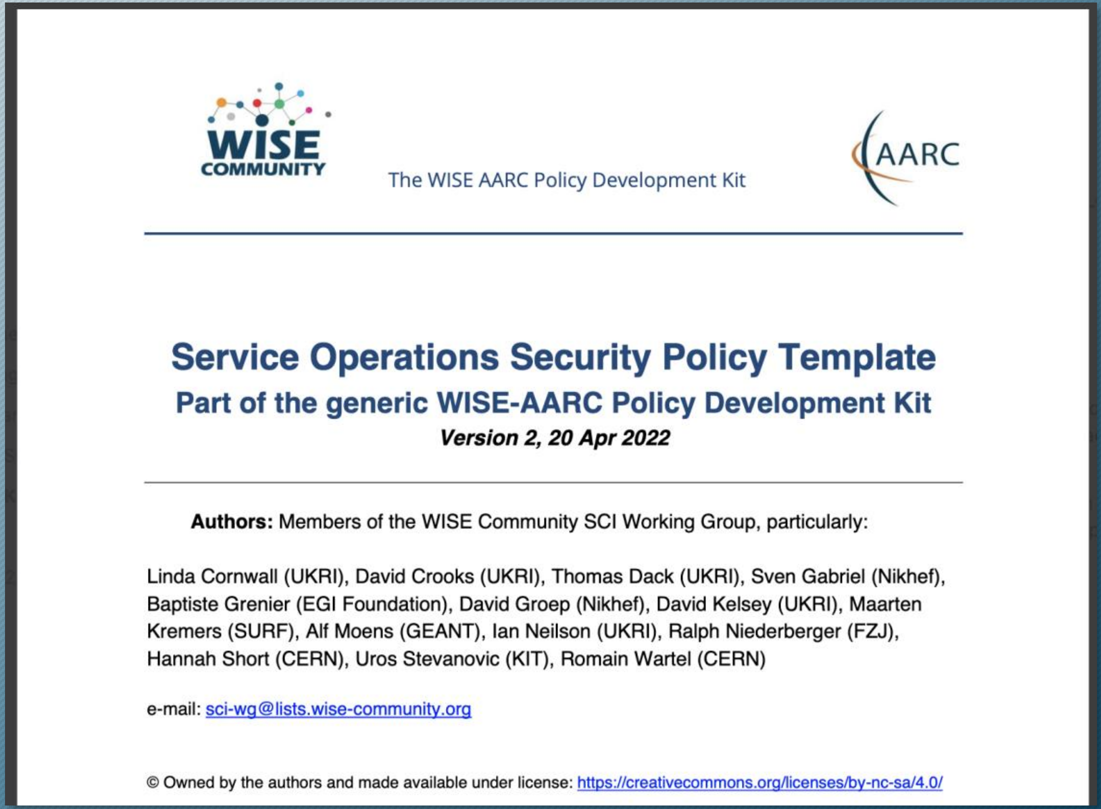
Policy Area	New Template	Lead Participants
Top Level	Infrastructure Policy	IRIS
Data Protection	Privacy Statement	WLCG, IRIS
Data Protection	Policy on the Processing of Personal Data	EGI, WLCG
Membership	Community Policy	IRIS, EOSC, GN5-1, IGTF
Membership	Acceptable Authentication Assurance	GN5-1, IGTF
Operational Security	Incident Response	eduGAIN, Sirtfi, GN5-1, EOSC & many opsec groups
Operational Security	Service Operations	EOSC, IRIS

Service Operations Security Policy

- Original AARC PDK Template: https://docs.google.com/document/d/1_cNMF3l3YVPqBBH0MPqx9DLAL1t3Z33_fJcjln8Xk48/edit#heading=h.idp93lqbm8kt
- In the UK, the IRIS Infrastructure used the PDK template – but made many changes to simplify and improve its Service Operations Security Policy (approved May 2021)
- The SCI working group used the IRIS version together with input from EOSC-hub, EOSC Future, EGI, ELIXIR, HIFIS and worked from October 2021 to April 2022
- See https://wiki.geant.org/display/WISE/Policy+Development+Kit
- The EOSC Security Baseline (Sep 2022) may serve as a better option for loosely coupled federations
- https://wiki.eoscfuture.eu/display/PUBLIC/EOSC+Security+Operational+Baseline
- EOSC FAQ Guidance at: https://wiki.eoscfuture.eu/display/EOSCF/EOSC+Security+Operational+Annotated+Baseline

Service Operations Security Policy

WISE PDK Template Version 2 See *WISE-SCI-PDK-ServiceOpsSecPol-V2.pdf*



The WISE AARC Policy Development Kit

Service Operations Security Policy Template

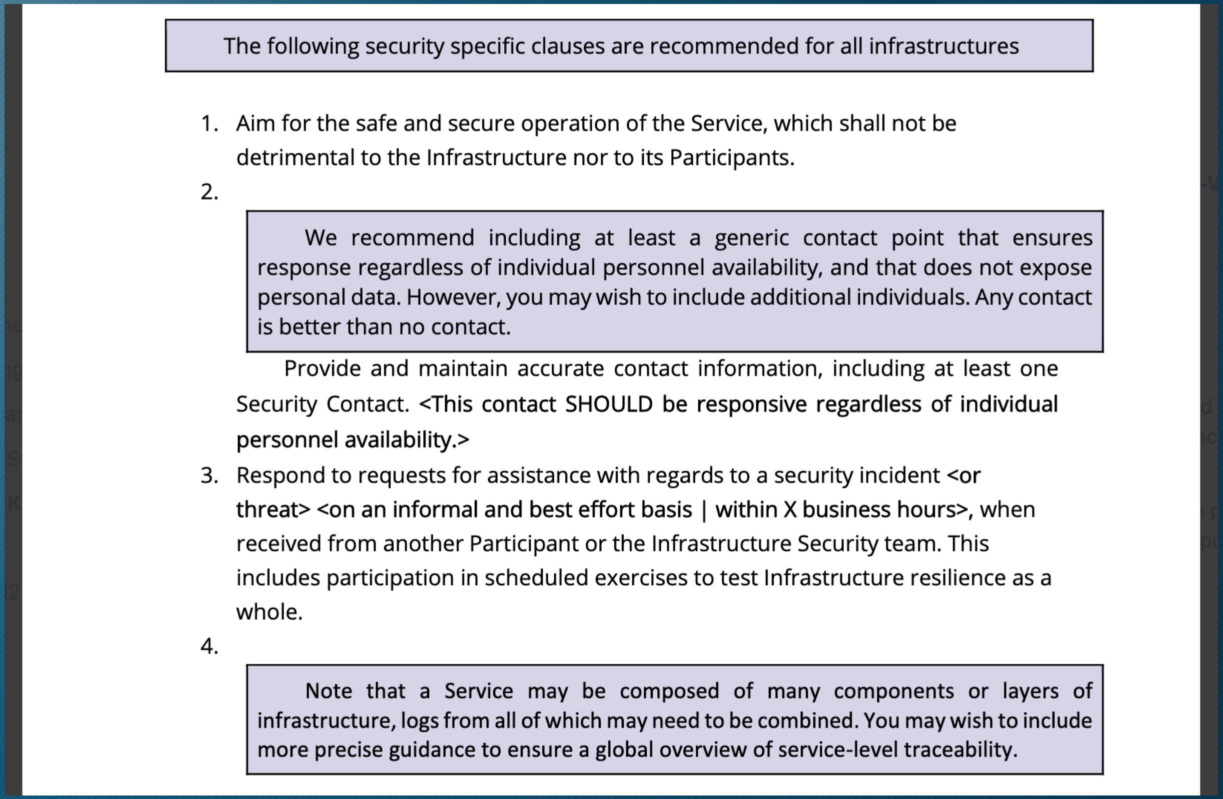
Part of the generic WISE-AARC Policy Development Kit

Version 2, 20 Apr 2022

Authors: Members of the WISE Community SCI Working Group, particularly:

Linda Cornwall (UKRI), David Crooks (UKRI), Thomas Dack (UKRI), Sven Gabriel (Nikhef), Baptiste Grenier (EGI Foundation), David Groep (Nikhef), David Kelsey (UKRI), Maarten Kremers (SURF), Alf Moens (GEANT), Ian Neilson (UKRI), Ralph Niederberger (FZJ), Hannah Short (CERN), Uros Stevanovic (KIT), Romain Wartel (CERN)

e-mail: sci-wg@lists.wise-community.org



The following security specific clauses are recommended for all infrastructures

1. Aim for the safe and secure operation of the Service, which shall not be detrimental to the Infrastructure nor to its Participants.
2. We recommend including at least a generic contact point that ensures response regardless of individual personnel availability, and that does not expose personal data. However, you may wish to include additional individuals. Any contact is better than no contact.

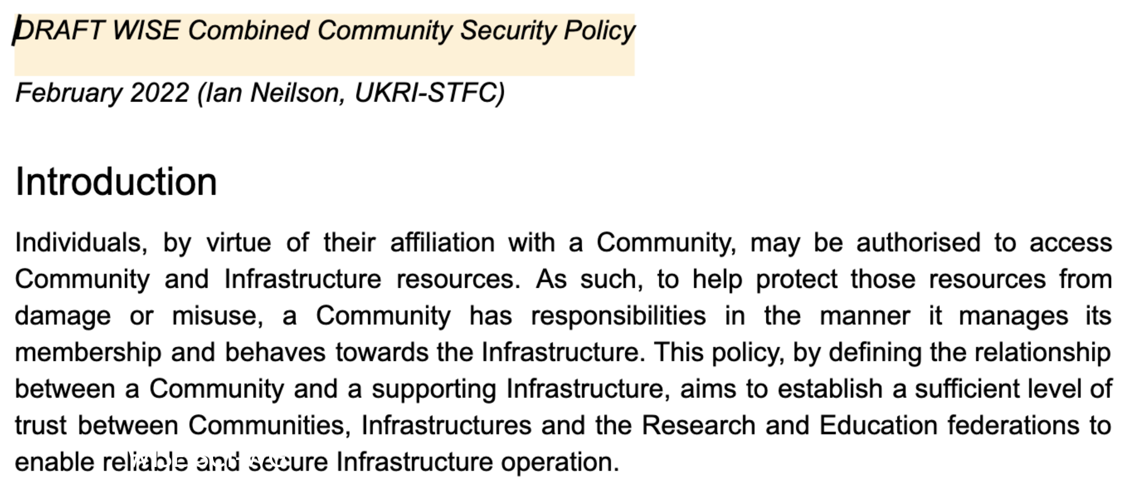
   Provide and maintain accurate contact information, including at least one Security Contact. <This contact SHOULD be responsive regardless of individual personnel availability.>
3. Respond to requests for assistance with regards to a security incident <or threat> <on an informal and best effort basis | within X business hours>, when received from another Participant or the Infrastructure Security team. This includes participation in scheduled exercises to test Infrastructure resilience as a whole.
4. Note that a Service may be composed of many components or layers of infrastructure, logs from all of which may need to be combined. You may wish to include more precise guidance to ensure a global overview of service-level traceability.

Data Protection and GDPR

- AARC PDK – old template: *https://docs.google.com/document/d/1QseGQVzUQqvosqhjkF2qlHUI4Swlhgb8oDe8N6NWcqE/edit*
- Updated “Processing of Personal Data Policy Framework” has been worked on
  - During 2022 in the WISE SCI-WG
  - Failed to reach consensus – so given up for now
  - Minimising risks (AARC PDK guidance) is not accepted by the working group
  - Developing new “contentious” policy has been found to be difficult over Zoom
- We were also waiting/hoping for the new **GEANT DP Code of Conduct version 2**
  - This did not happen and will not – now just best practice/guidance
    - And not for transfers outside of the EU
- Work will continue in 2023

Community Combined Security Policy – new PDK template (work in progress)

- IRIS (UK) has produced new policy (awaiting approval – April 2023)
- Based on combining two policies (AARC PDK & EGI security policy)
  - Community Membership Management Policy & VO Operations Policy
- *WISE SCI-WG PDK work in progress*

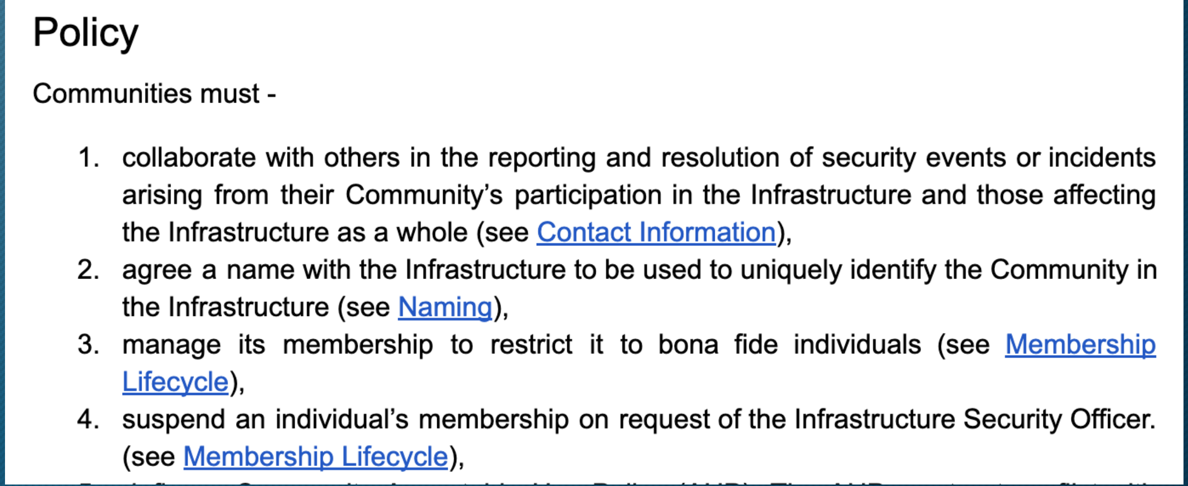


DRAFT WISE Combined Community Security Policy

February 2022 (Ian Neilson, UKRI-STFC)

Introduction

Individuals, by virtue of their affiliation with a Community, may be authorised to access Community and Infrastructure resources. As such, to help protect those resources from damage or misuse, a Community has responsibilities in the manner it manages its membership and behaves towards the Infrastructure. This policy, by defining the relationship between a Community and a supporting Infrastructure, aims to establish a sufficient level of trust between Communities, Infrastructures and the Research and Education federations to enable reliable and secure Infrastructure operation.



Policy

Communities must -

1. collaborate with others in the reporting and resolution of security events or incidents arising from their Community's participation in the Infrastructure and those affecting the Infrastructure as a whole (see Contact Information),
2. agree a name with the Infrastructure to be used to uniquely identify the Community in the Infrastructure (see Naming),
3. manage its membership to restrict it to bona fide individuals (see Membership Lifecycle),
4. suspend an individual's membership on request of the Infrastructure Security Officer. (see Membership Lifecycle),

The future: WISE & SCI in 2023

- WISE work continues within the working groups
- SCI-WG
  - Will restart meetings soon
  - Will continue to work on updated policy templates from AARC PDK
    - Data Protection and GDPR
    - Community Security Policies
- Full WISE Community meetings still to be defined for 2023
  - Looks difficult to find a free time for a European WISE meeting before summer holidays
    - To be decided
  - Plans underway to propose a WISE meeting in the USA at the NSF Cybersecurity Summit
    - October 24-26 2023, LBNL, Berkeley, CA
- Please join the WISE mail list (all welcome)
  - *https://lists.wise-community.org/sympa/info/wise*

More information

The original AARC PDK: https://aarc-community.org/policies/policy-development-kit/

- AARC guidance documents on policy: https://aarc-project.eu/guidelines/#policy

WISE Community: https://wise-community.org/

- WISE SCI-WG – Wiki - https://wiki.geant.org/display/WISE/SCI-WG
- WISE SCI-WG PDK updates - https://wiki.geant.org/display/WISE/Policy+Development+Kit

Join WISE mail list: https://lists.wise-community.org/sympa/info/wise
Join WISE SCI-WG: https://lists.wise-community.org/sympa/subscribe/sci-wg

Questions?

- And discussion ….

Backup slides

WISE Mission - reminder

- *The WISE Community enhances best practice in information security for IT infrastructures for research.*
- *How? Through membership of working groups and attendance at workshops the members participate in the joint development of policy frameworks, guidelines, and templates.*

Endorsement of SCI Version 2 at TNC17 (Linz)

- 1st June 2017
- *Infrastructures endorse the governing principles and approach of SCI, as produced by WISE, as a medium of building trust between infrastructures, to facilitate the exchange of security information in the event of a cross-infrastructure incident, and the collaboration of e-Infrastructures to support the process. These Infrastructures welcome the development of an information security community for the Infrastructures, and underline that the present activities by the research and e-Infrastructures should be continued and reinforced*
- Endorsements have been received from the following infrastructures; EGI, EUDAT, GEANT, GridPP, MYREN, PRACE, SURF, WLCG, XSEDE, HBP
- https://www.geant.org/News_and_Events/Pages/supporting-security-for-collaborating-infrastructures.aspx

SCIv2 assessment in practice

- UK IRIS infrastructure use-case completed
- Some (personal – Ian Neilson) observations and questions –
  - ‘Good in parts’ infrastructure – how to score?
    - weakest, best, average …. ?
  - “Checks” are definitely not standalone
    - how much do checks help?
    - IRIS assessors very familiar with SCIv2 …
  - Is yet more guidance needed on ‘score’ interpretation?
  - Requirements ‘creeping’ into the assessment
    - e.g. central logging is a scored item ….. but not mentioned in SCIv2.
  - Edits still needed
    - e.g. not useful to refer to AARC templates in the checks.